

Security & Hacking

By / Ahmed Wael

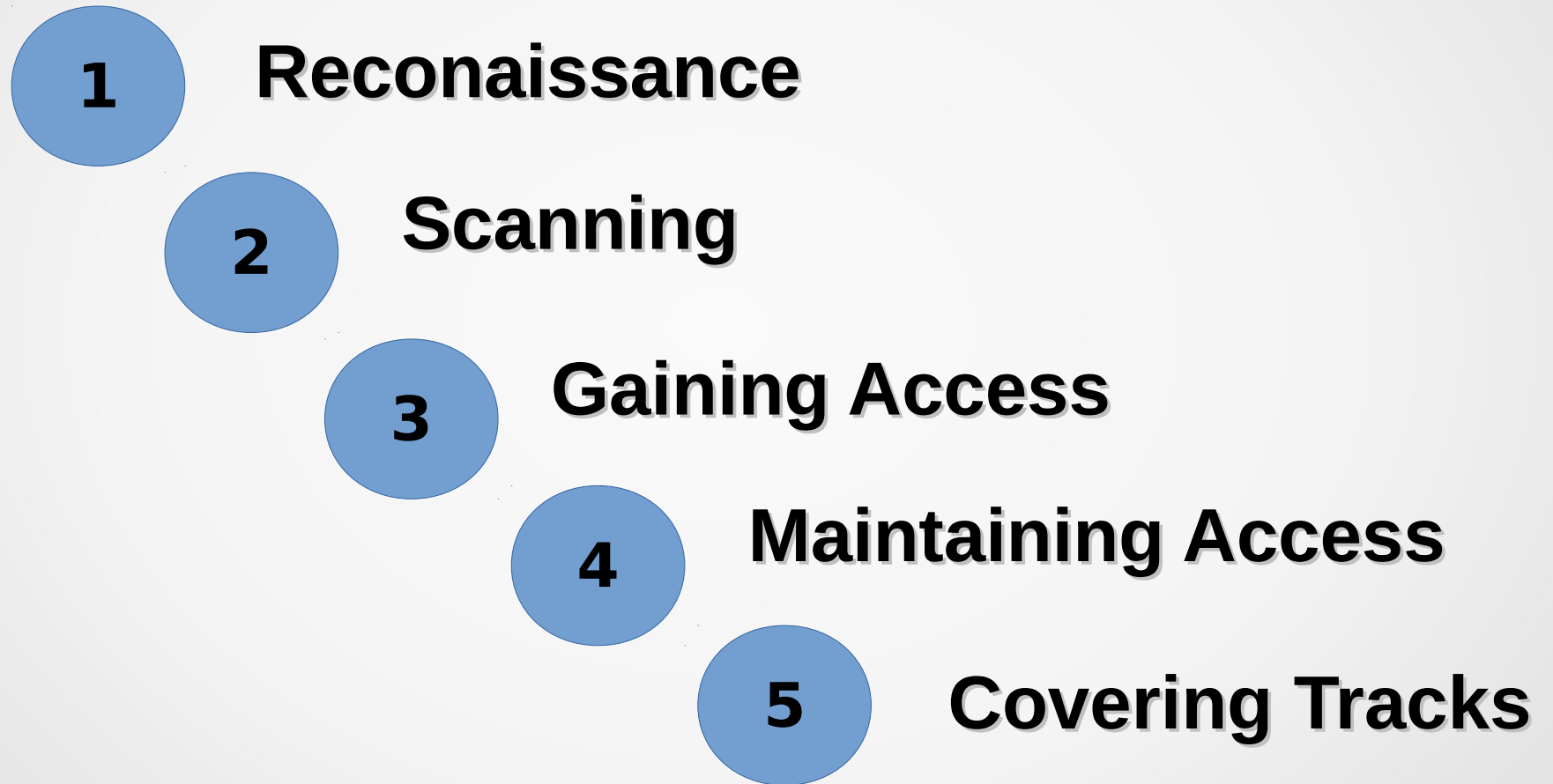
Introduction

- **Who are Hackers ?**

Intelligent individuals with ,excellent computer skills with the ability to create and explore into the computer's software and hardware



Hacking Cycle



Hackers classification

Black Hats

- Individuals with extraordinary computing skills, resorting to malicious or destructive activities. Also known as crackers



White Hats

- Individuals professing hacker skills and using them for defensive purposes. Also known as security analysts



Gray Hats

- Individuals who work both offensively and defensively at various times



Suicide Hackers

- Individuals who aim to bring down critical infrastructure for a "cause" and are not worried about facing 30 years in jail for their actions



Ethical Hacking

Ethical hackers try to answer the following questions:

- What can the intruder see on the target system? (Reconnaissance and Scanning phases)
- What can an intruder do with that information? (Gaining Access and Maintaining Access phases)
- Does anyone at the target notice the intruders' attempts or successes? (Reconnaissance and Covering Tracks phases)

Threats



Virus

Virus is a self-replicating program that produces its own code by attaching copies of itself into other executable codes



Virus

Hide itself from Detection By

Encryption

Redirection



Indication of Virus Attack

Programs take longer to load than the normal
Computer's hard drive constantly runs out of free
Space

Files have strange names which are not
recognizable

Programs act erratically

Resources are used up



Worm

A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs

**A virus requires some kind of human interaction
A Worm doesn't**



Backdoor

Backdoors are network utilities that enable an attacker to exercise unauthorized remote control of the infected computers on a network



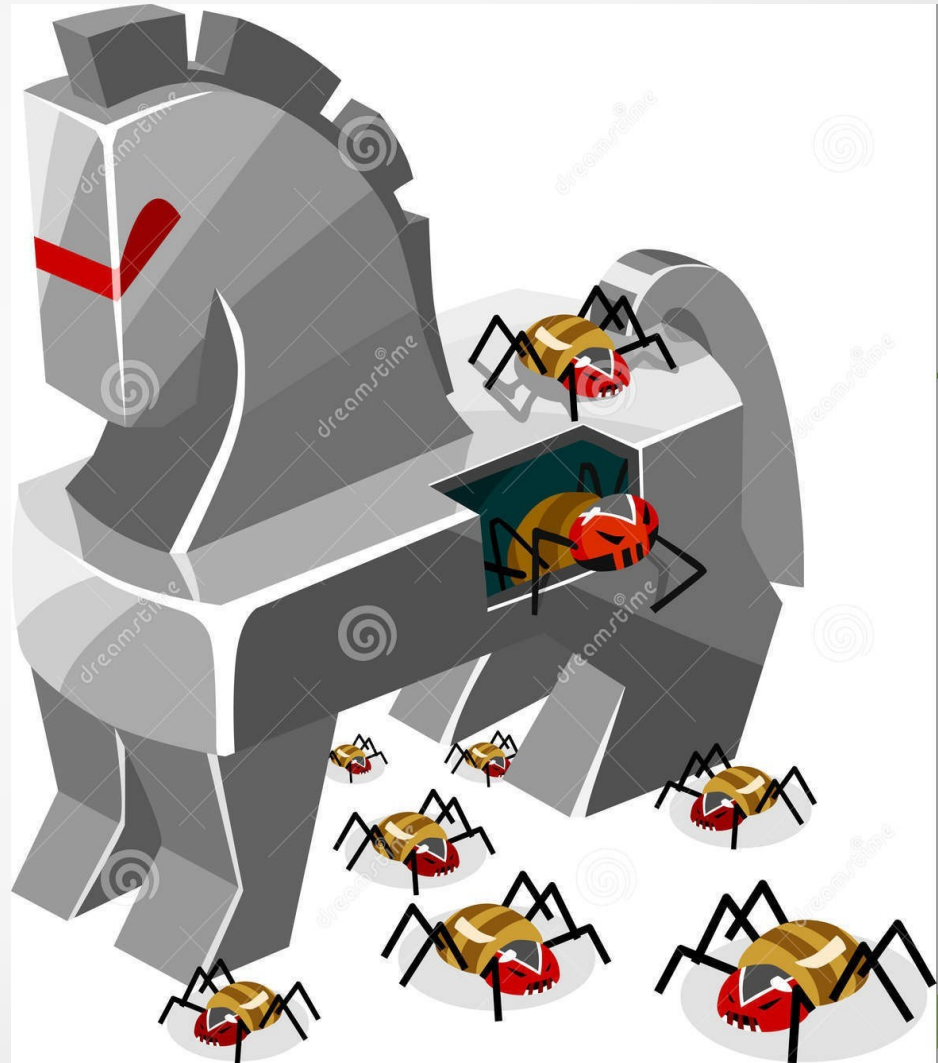
Backdoor

They allow an attacker to access almost everything on the affected computer such as steal data from it, upload, erase information, etc



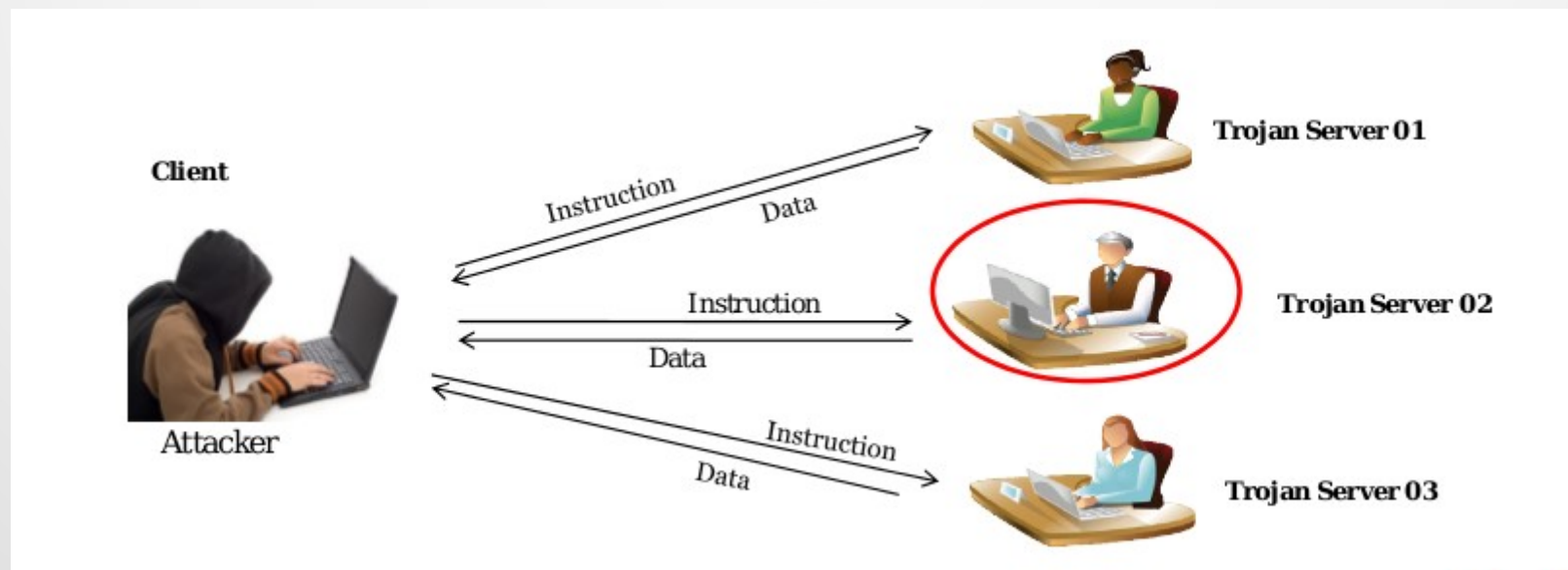
Trojan

Trojan horse is a program in which the malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on your hard disk



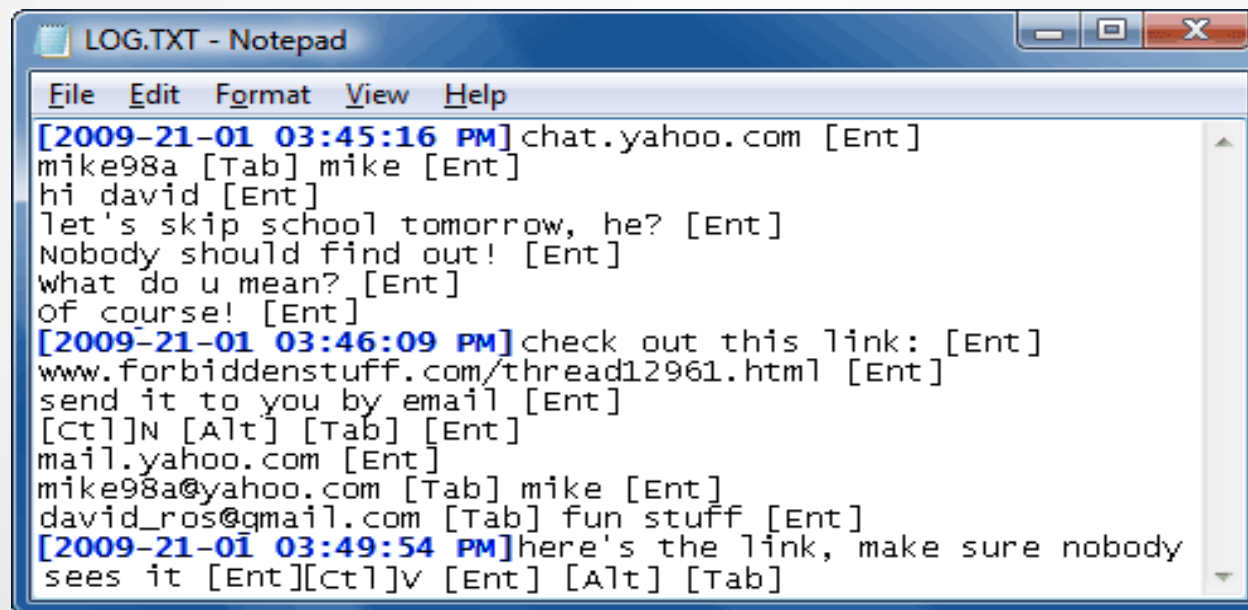
Trojan effect

With the help of a Trojan, an attacker gets access to the stored passwords in the Trojaned computer and would be able to read personal documents, delete files and display pictures, and/or show messages on the screen



Keylogger

The action of recording (or logging) the keys struck on a keyboard



```
LOG.TXT - Notepad
File Edit Format View Help
[2009-21-01 03:45:16 PM] chat.yahoo.com [Ent]
mike98a [Tab] mike [Ent]
hi david [Ent]
let's skip school tomorrow, he? [Ent]
Nobody should find out! [Ent]
what do u mean? [Ent]
of course! [Ent]
[2009-21-01 03:46:09 PM] check out this link: [Ent]
www.forbiddenstuff.com/thread12961.html [Ent]
send it to you by email [Ent]
[Ctrl]N [Alt] [Tab] [Ent]
mail.yahoo.com [Ent]
mike98a@yahoo.com [Tab] mike [Ent]
david_ros@gmail.com [Tab] fun stuff [Ent]
[2009-21-01 03:49:54 PM] here's the link, make sure nobody
sees it [Ent][Ctrl]V [Ent] [Alt] [Tab]
```

How Does Antivirus Software Work ?

Most of the commercial antivirus software uses **two** techniques:

- Uses **virus dictionary** to look for known viruses while examining files
- Detects **suspicious behavior** from any computer program



Virus Dictionary Approach

- While examining the files the antivirus software refers to the dictionary of known viruses identified by the author of antivirus software
- If a bit of code in the file matches with that of any virus in the dictionary, then the antivirus software can either delete the file, repair the file by removing the virus, or quarantine it



Suspicious Behavior Approach

- The antivirus software monitors the behavior of all the programs instead of identifying the known viruses
- Whenever a program with suspicious behavior is found the software alerts the user and asks what to do



Other Ways to Detect Viruses

- Antivirus software will try to emulate the beginning of each new executable code that is being executed before transferring control to the executable
- If the program seems to be a virus or using self-modifying code then it immediately examines the other executable programs



Social engineering

There is no patch to human stupidity

Social engineering is the art of convincing people to reveal confidential information



Social engineering

Social Engineering Example



“ Hi, we are from CONSESCO Software. We are hiring new people for our software development team. We got your contact number from popular job portals. Please provide details of your job profile, current project information, social security number, and your residential address. ”

Social engineering

Criminal as Phone Banker



“ Hi, I am Mike calling from CITI Bank. Due to increasing threat perception, we are updating our systems with new security features. Can you provide me your personal details to verify that you are real Stella.

Thanks Mike, Here are my details. Do you need anything else? ”

Social engineering

Technical Support Example



“

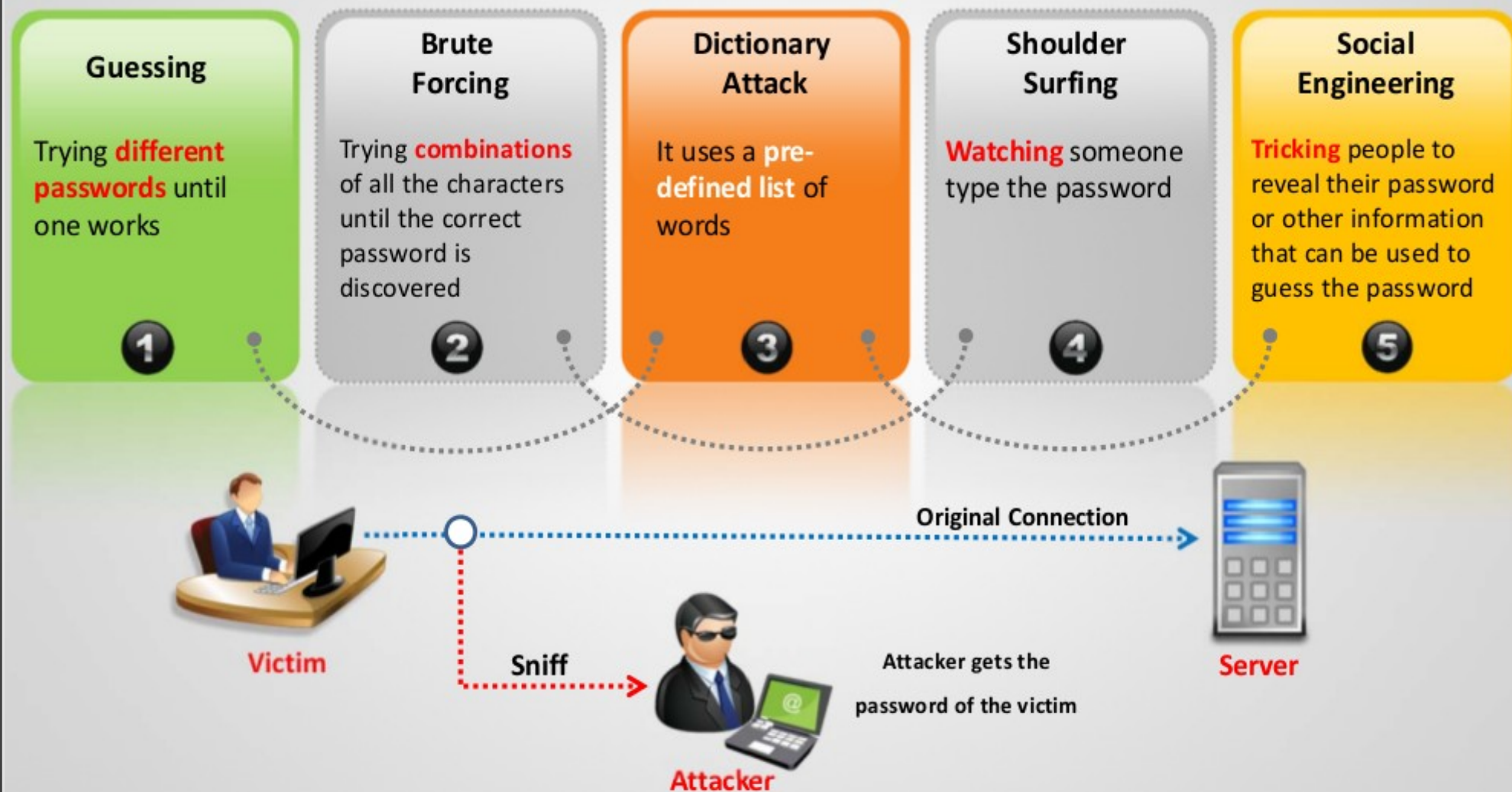
A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him.

The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker clear entrance into the corporate network

”

Password Cracking

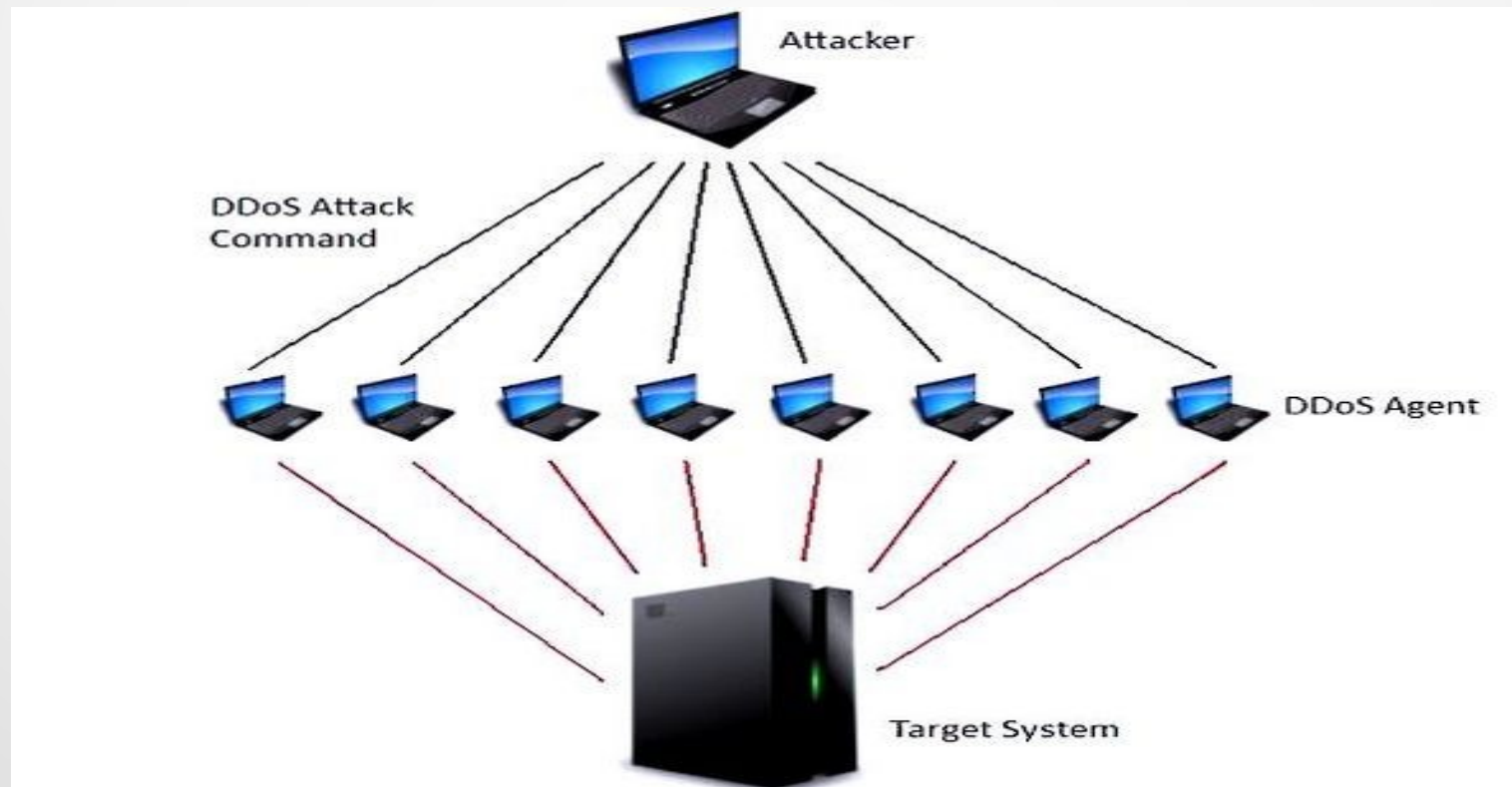
Password cracking is the process of **identifying** or **recovering** an unknown or forgotten password



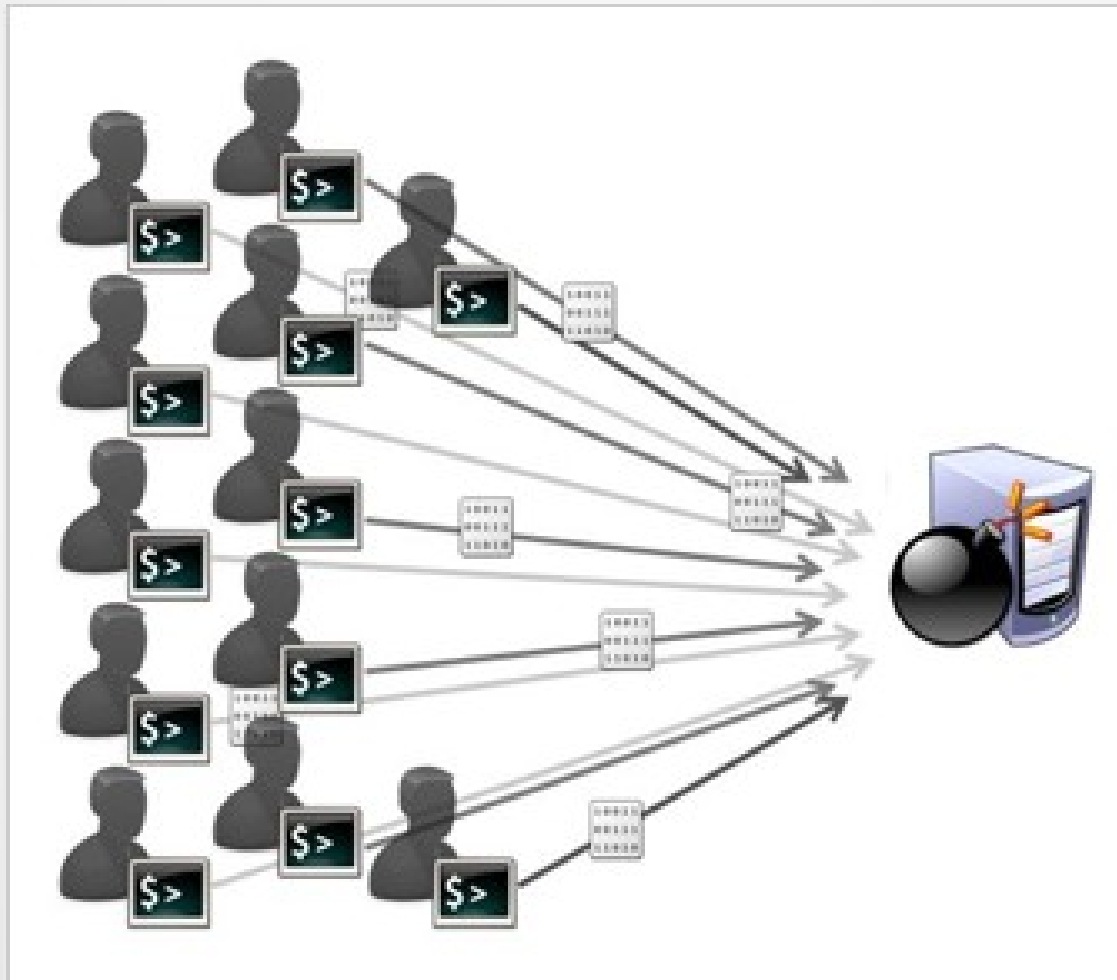
Denial of Service (DoS)

Targets system Availability

Could render the system unusable or slow it down by using it's resources



Denial of Service (DoS)



Live Denial of Service

Digital Attack Map Top daily DDoS attacks worldwide

[Map](#) · [Gallery](#) · [Understanding DDoS](#) · [FAQ](#) · [About](#) · [g+](#) [t](#) [f](#)

May 10

2015

Showing All Countries

Show Attacks



Large

Unusual

Combined

Large attacks on France, Czech Republic, Australia, + 10 others

Color Attacks By

Type

Duration

● TCP Connection

● Volumetric

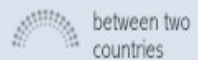
● Fragmentation

● Application

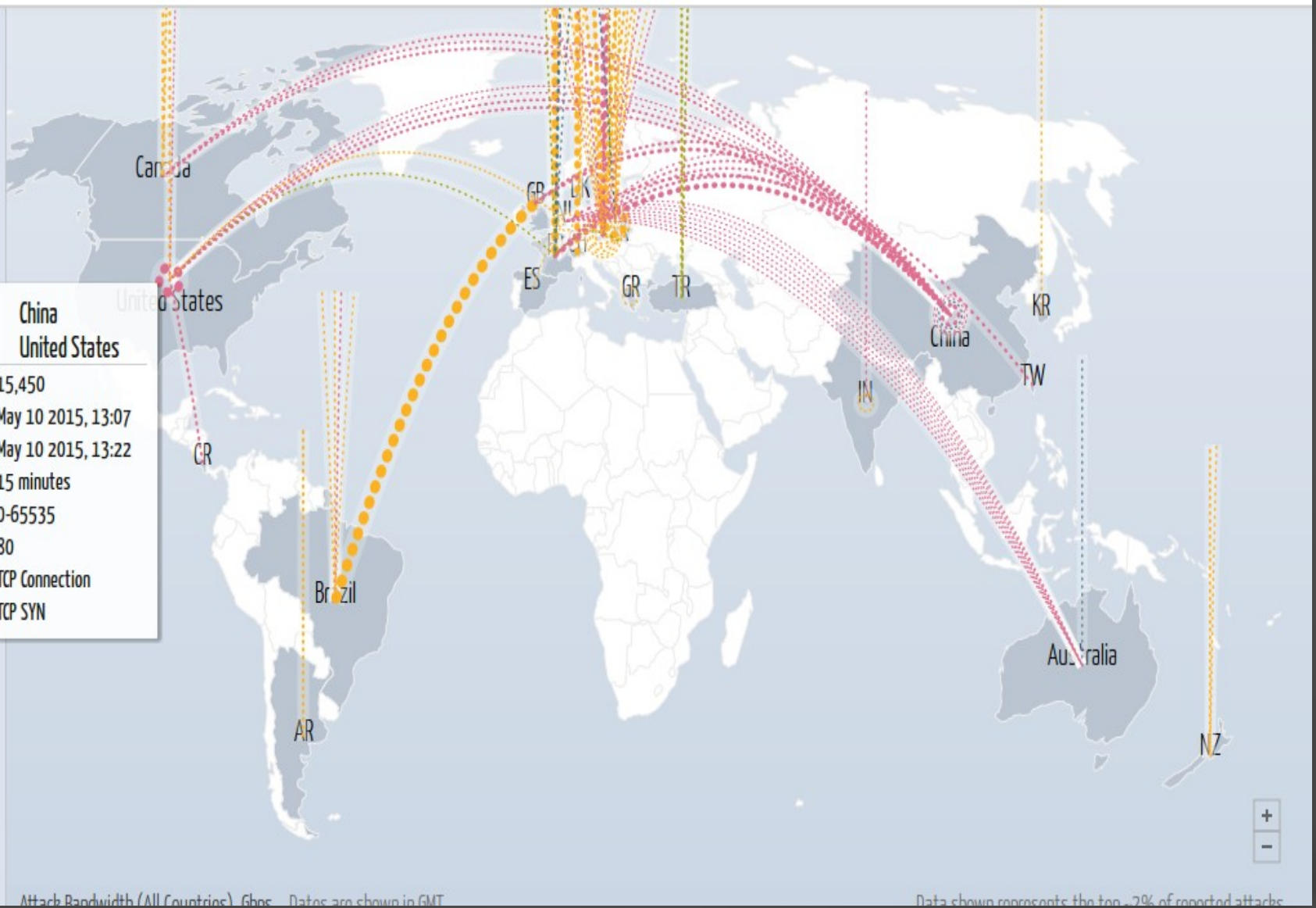
Size (Bandwidth, in Gbps)



Shape (source + destination)



Source	China
Destination	United States
Max Mbps	15,450
Start (GMT)	May 10 2015, 13:07
End (GMT)	May 10 2015, 13:22
Duration	15 minutes
Source Ports	0-65535
Dest. Ports	80
Class	TCP Connection
Subclass	TCP SYN

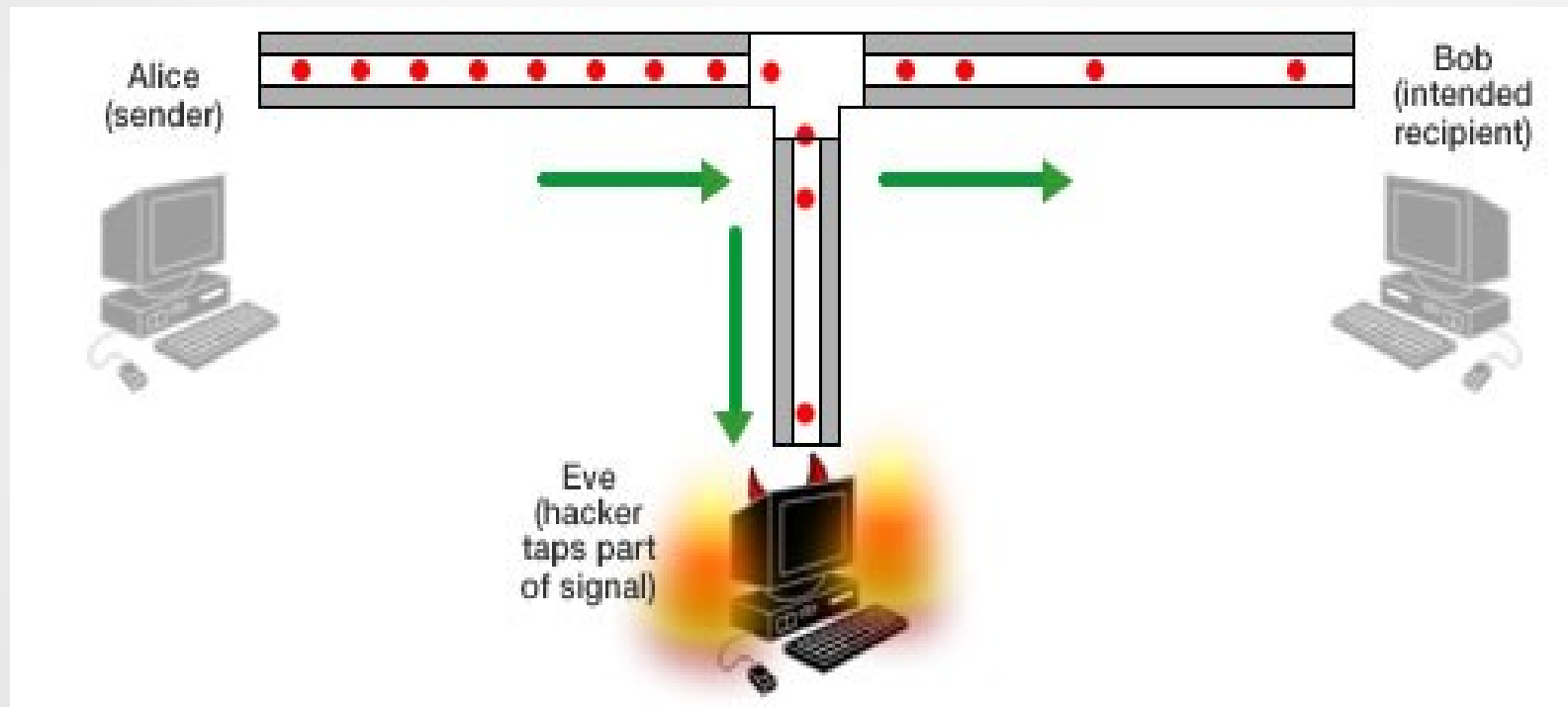


Eavesdropping

Unauthorized real-time interception of private communications such as phone calls and instant messages



Eavesdropping



Mobile Security

IMEI Number

International Mobile Equipment Identity (IMEI) is a number unique to every mobile phone

IMEI is a 15 digit number and is usually found printed inside the battery compartment of the phone

It can also be displayed on phone's screen by entering *#06#

It is used to deactivate the phone if it is stolen or lost



Note: The *#06# does not work for all mobile phones

Mobile Security procedures

❖ Patch mobile platforms and applications

❖ Avoid mobile device theft

❖ Use power-on authentication

❖ Regularly back up important data

❖ Use encryption to secure data in a mobile device

❖ Enable auto-lock feature

❖ Install only signed applications

❖ Install mobile phone antivirus

❖ Secure Bluetooth connectivity



Mobile Security

What to Do if Your **Mobile** is **Lost or Stolen?**



Use anti-theft software to remotely wipe the data and make the device unusable



Inform the local police and file First Information Report (FIR)



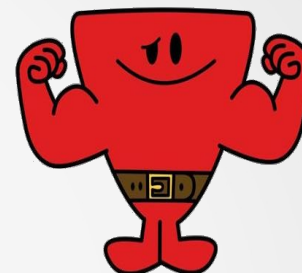
Contact the service provider and tell them to cancel the SIM card

Claim the mobile phone insurance to replace the cost of the handset

Protecting Yourself from Cyber Attacks

Delete all applications you don't use

Make Unique and Strong Password for Each Account



Go Only to Secured Websites (begin with httpS)

Cover Your Webcam (using Sticky Notes)

Do Not Respond to Emails from Strangers

Take Data Back-Ups on Regular Basis

Protecting Yourself from Cyber Attacks

Lock Your Computer and Phone When You Don't Use It

Never Reveal Any Financial Information via Telephone or Email

Update Your Anti-Virus



Never Open Attachments from Unknown Senders

Be Careful with What You Share on Social Media



Cyber Warfare

Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption



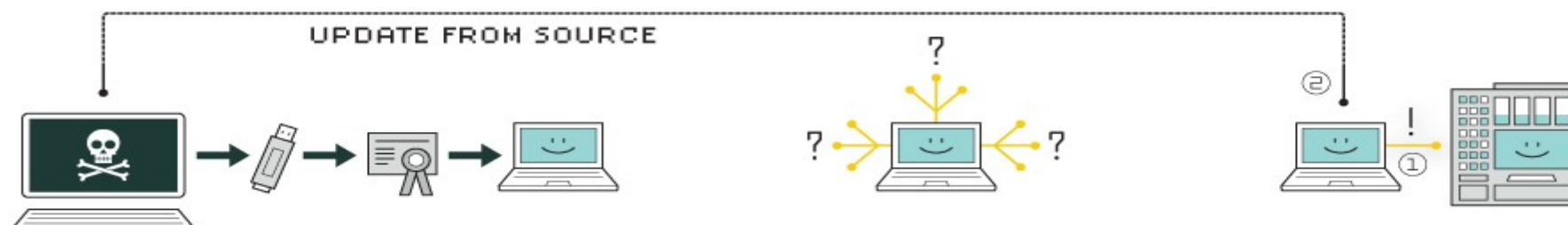
Cyber War Examples

Stuxnet

Stuxnet, a joint U.S.-Israel project, is known for reportedly destroying roughly a fifth of Iran's nuclear centrifuges by causing them to spin out of control

Cyber War Examples

HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Cyber War Examples

Turkey goes to stone ages

Iran stands accused of orchestrating a massive cyber attack on Turkey. Half of Turkey's provinces and 40 million people were plunged into the dark on March 31

Computers, airports, air traffic, traffic lights, hospitals, lights, elevators, refrigeration, water and sewage, everything simply stopped

The power outage lasted about 12 hours

Security Careers

Penetration Testing

Forensics Investigation

Incident Response

Malware Analysis

The End

Questions